PROFESSIONAL SERVICES

Creating Sustainable Business Advantage

BALTIMORE

www.baltimore.com

Certificate Policy and Certification Practice Statement Overview - Updated

July 6, 2000

Prepared for:
Ken Adrian
State of Iowa, IT Department
ITS 'B' Level, Hoover Building
Des Moines, IA 50319

Prepared by:
Professional Services
10 Fawcett Street
Cambridge, MA 02138

Table of Contents

1.0 Introduction

The Information Technology Department of the State of Iowa has requested that the Baltimore Technologies Professional Services Group provide an assessment of the facilities, technology, and documentation required for Iowa to implement recent legislation mandating the development of a public key infrastructure (PKI) for several state functions. Baltimore Technologies Professional Services has already submitted a PKI Needs Assessment and a PKI Architecture. This document addresses the documentation requirements that the State of Iowa must consider if it is going to operate, or contract for the operation of, a Certification Authority.

As was explained in the already-submitted Requirements Assessment and the upcoming PKI Architecture document, a Certification Authority (CA) is the heart of any PKI implementation. The CA is the instrument through which digital certificates are created, issued, and revoked in a PKI. The CA controls and is ultimately responsible for the operation of a PKI, although some functions, such as the Registration Authority, may be contracted-out to other entities.

The operation of a CA is not a trivial matter from operational, technical, legal, or liability standpoints. It is imperative that the operations of a CA and the PKI in general be set forth in documents that are accessible to and understandable by the users of a PKI. The two primary documents that attempt to provide the required knowledge to the users are known as a Certificate Policy (CP) and a Certification Practices Statement (CPS). While similar in format, the documents provide differing information. When combined, however, they lay the foundation for the successful operation of a CA and a PKI.

Baltimore Technologies Professional Services originally proposed to include a high-level summary of CP requirements and a PKI concept of operations in the first deliverable document, the Requirements Analysis. However, after further thought and discussion with the State of Iowa, it was decided that this information better belongs with the architecture study which is now being completed. The CP requirements, which are more legal or procedural in tone, are covered in this stand-alone document. The PKI concept of operations information, which is more technical, is covered in the PKI Architecture which will be delivered in a few days, particularly in the "Certification Process" section. Also included in the architecture document is much technical matter that may be of assistance in planning some other parts of a CP or CPS, such as identification and authentication functions, security controls, and certificate/CRL format.

Most CPs and the CPS' are prepared using a draft "standard" currently under development by the Internet Engineering Task Force. That framework, known generally as RFC 2527, was written by two well-known PKI technology experts several years ago. The intent of the authors was to provide a standard framework through which a CA could review the operational aspects of another CA and determine if cross-certification was possible between the CAs. Although RFC 2527 is in fact still a draft document, in the fast paced world of the Internet it has become the reference "standard" for virtually all CP and CPS development. RFC 2527 was written from a largely technical viewpoint and has been criticized for its lack of specificity in the coverage of such matters as liability and related legal issues. Nonetheless, most CP and CPS authors are able to adjust RFC 2527 as necessary to provide a useable product.

Normally, a CA prepares one CPS stating how it operates and one or more Certificate Policies that provide the details about a particular PKI application or type of certificate. However, there is no fixed formula that specifies either the relationship between a CP and a CPS or how many of

each type of document should be produced. These decisions need to be made by the operators of a CA or PKI after carefully considering the particular PKI implementation.

Clear documentation of how the PKI operates is an essential tool for any CA. However, there are varying approaches to the preparation and use of the CP and CPS. The role of the CPS can vary, depending on the contractual relationships (or lack thereof) between the parties to the PKI; or if the PKI is used exclusively for internal business or organization purposes. Regardless of the particular implementation, it is wise to draft these documents using clear and straightforward language.

2.0 Certificate Policy

A Certificate Policy is a document that is produced by either a CA or another body known as a Policy Administration Authority (PAA). Regardless of who produces it, the document sets forth what are in effect the requirements for the operation of a PKI. If prepared by a PAA, the CP sets the requirements that any CA participating in the PKI must meet in order to participate in the PKI managed by the PAA. If prepared by a CA, the CP explains what the CA does, while other documents (such as a CPS) describe how the CA functions.

There are two approaches to CP preparation. In the first, which may be preferable if only one CA will be issuing certificates, the CP is a shorter, high-level document that does not follow the RFC 2527 framework. Instead, it is composed of a limited number of sections that set forth the mission of the CA, the roles and responsibilities of the participants, the CA's security practices, and the applicable laws and regulations.

The second version of a CP is much longer and follows the RFC 2527 framework. It is frequently redundant of the CPS, as both documents are prepared under RFC 2527. This type of CP is most useful where there is a formal PAA setting the policy for a PKI and more than one CA will be providing services. In this scenario, the CP may be viewed as a "requirements" type of document, to which the CA responds with its CPS. For those who would like more background about Certificate Policies, Baltimore Technologies Professional Services recommends reviewing the Certification Authority Rating and Trust (CARAT) Guidelines published by the Internet Council of the National Automated Clearing House Association in January 2000, and available at http://www.nacha.org.

3.0 Certification Practice Statement

Unlike the CP, virtually every CPS in use today follows the RFC 2527 framework. A CPS is a much more technical document than a CP and explains in some detail how a CA operates. If there is a CP and more than one CA participating in a PKI operated by a formal PAA, the CPS may take the form of an answer to the requirements set forth in the CP. That is, the CPS explains to the PAA and the users of the PKI how its operations meet the requirements set forth in the CP. If only one CA is operating in a particular PKI, then the CPS will consist of a statement of that CA's operating practices and procedures.

For those who would like more information about Certification Practice Statements, Baltimore Technologies Professional Services recommends reviewing the Digital Signature Guidelines published by the Information Security Committee of the American Bar Association in August 1996, and available at http://www.abanet.org.

4.0 RFC 2527

RFC 2527 is a framework designed by two highly respected PKI technical experts for the Internet Engineering Task Force. The most recent version was released in March 1999. RFC 2527 attempts to provide an outline of all the information that the authors believed was necessary in order to prepare a CP or CPS. RFC 2527 consists of eight parts, each of which is explained below. The entire framework is included in Appendix A.

Most CP and CPS authors attempt to maintain the numbering scheme and section titles of RFC 2527. However, because several sections of the document in its current form are generally considered to be in need of revision, CP and CPS authors add and delete sections as necessary to fulfill the needs of the particular PKI implementation for which the CP or CPS is being prepared. It is not advisable to change the names of sections within RFC 2527 as one of the reasons for the document's development in the first place was to provide a means through which differing Certificate Policies and CPS' could be compared. Inserting different titles or information into the existing RFC 2527 framework defeats the reason for the framework.

Section 1 (Introduction) Described here are the scope and purpose of a Certificate Policy or CPS. Most important is the description of community and applicability; *i.e.*, the parties to whom the Certificate Policy or CPS will apply and the uses that will be permitted within the PKI.

Section 2 (General Provisions) This section address the obligations of the various parties to one another. The content of the provisions in this section will differ from one Certificate Policy or CPS to another, depending on the business and legal model used. This section also addresses matters related to enforcement of the parties' obligations, and issues such as the fees that may be charged, publication requirements, compliance audit requirements, and so forth.

Section 3 (Identification and Authentication) Addressed here is the central issue of confirmation of individual identity. Included are instructions regarding initial registration, the types of names that may be used in public key certificates, requests to renew expired or revoked certificates, and certain revocation requests.

Section 4 (Operational Requirements) Included here are high-level instructions regarding certain operations that are likely to occur in a PKI. Some of the more critical operations addressed include the issuance of certificates, their acceptance by Subscribers, and certificate revocation. This section also includes guidelines for Relying Parties concerning the need to check a certificate's current validity.

Section 5 (Physical, Procedural, and Personnel Security Controls) This section provides a high-level description of the various security mechanisms employed by a CA. For obvious reasons, details about the security mechanisms and procedures are not supplied, but the reader is given assurance that the CA is operated in a secure fashion. Those readers with a "need to know" may be given access to more detailed security documents.

Section 6 (Technical Security Controls) Provided here is information about technical issues such as key generation and control, and some additional security features not discussed in Section 5.

Section 7 (Certificate and Certificate Revocation List Profiles) This section provides highly technical information about the composition of the certificates and revocation lists (if any) used in the PKI.

Section 8 (Specification Administration) The final section provides information about how a CP or CPS may be amended and on how the CA will notify affected parties of those changes.

Appendix A

RFC 2527, IETF Draft CP and CPS Framework

1. INTRODUCTION
1.1 Overview
1.2 Identification
1.3 Community and Applicability
1.3.1 Certification authorities
1.3.2 Registration authorities
1.3.3 End entities
1.3.4 Applicability
1.4 Contact Details
1.4.1 Specification administration organization
1.4.2 Contact person
1.4.3 Person determining CPS suitability for the policy
2. GENERAL PROVISIONS
2.1 Obligations
2.1.1 CA obligations
2.1.2 RA obligations
2.1.3 Subscriber obligations
2.1.4 Relying Party obligations
2.1.5 Repository obligations
2.2 Liability
2.2.1 CA liability
2.2.2 RA liability
2.3 Financial responsibility
2.3.1 Indemnification by Relying Parties
2.3.2 Fiduciary relationships
2.3.3 Administrative processes
2.4 Interpretation and Enforcement
2.4.1 Governing law
2.4.2 Severability, survival, merger, notice
2.4.3 Dispute resolution procedures
2.5 Fees
2.5.1 Certificate issuance or renewal fees
2.5.2 Certificate access fees
2.5.3 Revocation or status information access fees
2.5.4 Fees for other services such as policy information
2.5.5 Refund policy
2.6 Publication and Repository
2.6.1 Publication of CA information
2.6.2 Frequency of publication
2.6.3 Access controls
2.6.4 Repositories
2.7 Compliance audit
2.7.1 Frequency of entity compliance audit
2.7.2 Identity/qualifications of auditor